CLAIMS

1. A method of distributing data comprising:

(a) encrypting a plurality of data units each with one of a sequence of keys;

(b) communicating encrypted data units to a plurality of user terminals;

(c) communicating at least one seed value to a user terminal;

(d) generating from the seed value or values a sequence of keys greater in number than the number of seed values communicated to the user terminal; and

(e) decrypting data units at the user terminal using the said sequence of keys, characterised in that in step (d) a sequence of keys constituting an arbitrarily doubly bounded portion of the sequence of keys of step (a) is generated, and in that the position in sequence of the lower and upper bounds of the said portion are determined by the at least one seed value communicated in step (c).

2. A method according to claim 1, in which the sequence of keys used in step (a) is generated by:

(a) operating on one or more initial seed values and generating a greater number of intermediate seed values, which intermediate seed values blind the initial seed values:

(b) further operating on the values produced by the preceding step and generating thereby a still greater number of further values, which further values blind the values produced by the preceding step;

(c) iterating step (B) until the number of values produced is equal to or greater than the number of keys required for step (a).

3. A method according to claim 1 or 2, in which step (d) includes combining values derived from a plurality of different seed values.

4. A method according to claim 1 or 2 or 3, in which step (d) includes operating on a plurality of seed values with each of a plurality of different blinding functions.

5. A method according to Claim 4, including:

(I) operating on at least one root seed value with each of a set of different blinding functions thereby producing a plurality of further values;

(II) operating with each of the set of different blinding functions on the further values produced by the preceding step or on values derived therefrom;

(III) iterating step (II) and thereby producing, by the or each iteration, a next successive layer in a tree of values;

(IV) in step (a), using as the sequence of keys values derived from the sequence of seeds in one or more of the layers produced by step (III); and

(V) in step (c), communicating to a user terminal at least one value from within the body of the tree, the position in the tree of the or each value communicated to the user terminal thereby determining the position and extent of the portion of the sequence of keys available to the user for use in decrypting data units.

6. A method according to claim 5 including, in step (I)

(i) operating with the set of different blinding functions on plurality of different seed values

(ii) for each of the different blinding functions, combining the result of operating with one blinding function on one of the seed values and the result of operating with the same or another blinding function on another of the respective seed values, thereby producing a plurality of further values.

7. A method according to claim 3, in which step (d) includes

(I) combining first and second values derived from respective first and second blinding function chains, thereby producing a first next seed or key, the first and second blinding function chains having different respective seeds

(II) combining a value derived from a position in the first chain subsequent to the position of the first value and a value derived from a position in

the second chain preceding the position of the second value, thereby producing a further next seed or key value.

8. A method according to claim 7, including iterating step (ll) thereby producing further key values, in each iteration values from positions subsequent to the previous position in the first chain and preceding the previous position in the second chain being combined.

9. A method according to any one of the preceding claims in which the seed values are communicated to the user terminals, via a communications network.

10. A method according to claim 9 in which the seed values are communicated from a plurality of key management nodes to customer terminals.

11. A method of encrypting data for distribution comprising:

(a) operating on at least one root seed value with one or more blinding functions, thereby producing a plurality of further values;

(b) operating with one or more blinding functions on the further values produced by the preceding step or on values derived therefrom;

(c) iterating step (b) and thereby producing, by the or each iteration, a next successive layer in a tree of values;

(d) encrypting a plurality of data units using a sequence of key values derived from one or more of the layers generated by step (c).

12. A method of communicating data to a group of users comprising:

(a) encrypting data for distribution;

(b) systematically and independently of group membership changes changing a key used in encrypting the data for distribution;

(c) communicating the data to the users; and

(d) at the users' terminals decrypting the data, characterised by generating from a number of initial seed values a greater number of intermediate seed values, and deriving from the intermediate seed values the plurality of keys used in encrypting the data for distribution.

13. A method according to claim 12, in which every possible sub-set of the sequence of keys is derivable from a respective combination of seed values.

14. A method according to any of the preceding claims, in which each encrypted data unit carries an unencrypted index number to identify to any receiver which key in the sequence should be used to decrypt that data unit.

15. A method according to any of claims 1 to 14 where the seeds required by any receiver to construct the keys for a specific sub-range of the entire key sequence are communicated in an order that implicitly identifies each seed.

16. A method according to any of the preceding claims, in which multiple data senders use the same sequence of keys as each other to encrypt the same or different data units.

17. A method according to any of the preceding claims, in which each key in the sequence generated from the seeds is used as an intermediate key to be combined with another intermediate key or sequence of keys to produce a sequence of keys to encrypt or decrypt the data units.

18. A method of distributing data comprising encrypting a plurality of data units each with one of a sequence of keys and communicating the encrypted data units to a plurality of user terminals, characterised in that the sequence of keys is generated and allocated to application data units in accordance with a key construction algorithm, and in that copies of the key construction algorithm are distributed to a plurality of key managers so that, in use, receivers may obtain keys for access to an arbitrary portion of the data from a key manager without reference to any data sender or senders.

19. A method of operating a user terminal comprising:

a) receiving a plurality of data units encrypted with a sequence of keys;

b) receiving one or more seed values;

c) generating from the one or more seed values an arbitrarily doubly bounded key sequence larger in number than the number of seeds received in step (b); and

d) decrypting the application data units using the values generated in step (c) or values derived therefrom.

20. A key manager comprising means arranged to operate in accordance with the method of claim 18.

21. A customer terminal comprising means arranged to operate in accordance with the method of claim 19.

22. A communications network comprising means arranged to operate by method in accordance with the method of any one of claims 1 to 19.

23. A network according to claim 22, in which the data is distributed using a multicast or broadcast transmission mode.

24. A network according to claim 22 or 23, in which the network includes a virtual private network (VPN) and in which different combinations of seeds for constructing different sub-ranges of keys for decrypting data give members of the virtual private network different periods of access to the VPN.

25. A data carrier storing a plurality of data units encrypted for use in a method according to any one of claims 1 to 19.